

An Optimal Lower Bound for the Frobenius Problem

by Iskander Aliev (Edinburgh) and Peter M. Gruber (Vienna)

Abstract. Given $N \geq 2$ positive integers a_1, a_2, \dots, a_N with $\text{GCD}(a_1, \dots, a_N) = 1$, let f_N denote the largest natural number which is not a positive integer combination of a_1, \dots, a_N . This paper gives an optimal lower bound for f_N in terms of the absolute inhomogeneous minimum of the standard $(N - 1)$ -simplex.

Keywords: absolute inhomogeneous minimum, covering constant, lattice, simplex.

2000 MS Classification: 11D85, 11H31, 52C17

1 Introduction and statement of results

Given $N \geq 2$ positive integers a_1, a_2, \dots, a_N with $\text{GCD}(a_1, \dots, a_N) = 1$, the Frobenius problem asks for the largest natural number $g_N = g_N(a_1, \dots, a_N)$ (called the Frobenius number) such that g_N has no representation as a non-negative integer combination of a_1, \dots, a_N . In this paper, without loss of generality, we assume that $a_1 < a_2 < \dots < a_N$. The simple statement of the Frobenius problem makes it attractive and the relevant bibliography is very large (see [14] and Problem C7 in [9]). We will mention just few main results.

For $N = 2$, the Frobenius number is given by an explicit formula due to W. J. Curran Sharp [3]:

$$g_2(a_1, a_2) = (a_1 - 1)(a_2 - 1) - 1.$$

The case $N = 3$ was solved explicitly by Selmer and Beyer [20], using a continued fraction algorithm. Their result was simplified by Rödseth [15] and later by Greenberg [8]. No general formulas are known for $N \geq 4$. Upper bounds, among many others, include classical results by Erdős and Graham [5]

$$g_N \leq 2a_N \left[\frac{a_1}{N} \right] - a_1,$$

by Selmer [19]

$$g_N \leq 2a_{N-1} \left[\frac{a_N}{N} \right] - a_N,$$

and by Vitek [21]

$$g_N \leq \left\lceil \frac{(a_2 - 1)(a_N - 2)}{2} \right\rceil - 1,$$

as well as more recent results by Beck, Diaz, and Robins [2]

$$g_N \leq \frac{1}{2} \left(\sqrt{a_1 a_2 a_3 (a_1 + a_2 + a_3)} - a_1 - a_2 - a_3 \right),$$

and by Fukshansky and Robins [7], who produced an upper bound in terms of the covering radius of a lattice related to the integers a_1, \dots, a_N .

For $N = 3$, Davison [4] has found a sharp lower bound

$$g_3 \geq \sqrt{3a_1 a_2 a_3} - a_1 - a_2 - a_3,$$

where the constant $\sqrt{3}$ cannot be replaced by any smaller constant. Rödseth [15] proved in the general case that

$$g_N \geq ((N-1)! a_1 \cdots a_N)^{1/(N-1)} - \sum_{i=1}^N a_i.$$

The present paper gives a sharp lower bound for the function

$$f_N(a_1, \dots, a_N) = g_N(a_1, \dots, a_N) + \sum_{i=1}^N a_i$$

(and thus for g_N) in terms of a geometric characteristics of the standard $(N-1)$ -simplex. Clearly, $f_N = f_N(a_1, \dots, a_N)$ is the largest integer which is not a *positive* integer combination of a_1, \dots, a_N .

Following the geometric approach developed in [12] and [13], we will make use of tools from the geometry of numbers. Recall that a family of sets in \mathbb{R}^{N-1} is a *covering* if their union equals \mathbb{R}^{N-1} . Given a set S and a lattice L , we say that L is a *covering lattice* for S if the family $\{S+\mathbf{l} : \mathbf{l} \in L\}$ is a covering. Recall also that the *inhomogeneous minimum* of the set S with respect to the lattice L is the quantity

$$\mu(S, L) = \inf\{\sigma > 0 : L \text{ a covering lattice of } \sigma S\}$$

and the quantity

$$\mu_0(S) = \inf\{\mu(S, L) : \det L = 1\}$$

is called the *absolute inhomogeneous minimum* of S . If S is bounded and has inner points, then $\mu_0(S)$ does not vanish and is finite (see [11], Chapter 3).

Let S_{N-1} be the standard simplex given by

$$S_{N-1} = \{(x_1, \dots, x_{N-1}) : x_i \geq 0 \text{ reals and } \sum_{i=1}^{N-1} x_i \leq 1\}.$$

The main result of the paper shows that the constant $\mu_0(S_{N-1})$ is a sharp lower bound for (suitably normalized) Frobenius number and integers with relatively small f_N are, roughly speaking, dense in \mathbb{R}^{N-1} .

Theorem 1.1. (i) *For $N \geq 3$ the inequality*

$$\mu_0(S_{N-1}) \leq \frac{f_N(a_1, \dots, a_N)}{(a_1 \cdots a_N)^{1/(N-1)}} \quad (1)$$

holds.

(ii) *For any $\epsilon > 0$ and for any point $\alpha = (\alpha_1, \dots, \alpha_{N-1})$ in \mathbb{R}^{N-1} there exist N integers $0 < a_1 < a_2 < \dots < a_N$ with $\text{GCD}(a_1, \dots, a_N) = 1$ such that*

$$\left| \alpha_i - \frac{a_i}{a_N} \right| < \epsilon, \quad i = 1, 2, \dots, N-1 \quad (2)$$

and

$$\frac{f_N(a_1, \dots, a_N)}{(a_1 \cdots a_N)^{1/(N-1)}} < \mu_0(S_{N-1}) + \epsilon. \quad (3)$$

Remark 1.1. Prof. L. Davison kindly informed the authors that the part (i) of Theorem 1.1 was proved by Rödseth in [16] without using geometry of numbers.

The quantity $\mu_0(S)$ is closely related to the *covering constant* $\Gamma(S)$ of the set S , where

$$\Gamma(S) = \sup \{\det(L) : L \text{ a covering lattice of } S\}. \quad (4)$$

By Theorem 1, Ch. 3, §21 of [11] (see also [1]) for each Lebesgue measurable set S

$$\Gamma(S) \leq \text{vol}(S), \quad (5)$$

and by Theorem 2 ibid.

$$\mu_0(S) = \frac{1}{\Gamma(S)^{1/(N-1)}}. \quad (6)$$

The proof of Theorem 1, Ch. 3, §21 of [11] easily implies that the equality in (5) is attended only if S is a space-filler. Further, by Theorem 6.3 of [17], packings of simplices cannot be very dense and, consequently, S_{N-1} is not a space-filler. Therefore, by (5) and (6),

$$\mu_0(S_{N-1}) > \frac{1}{(\text{vol}(S_{N-1}))^{1/(N-1)}} = ((N-1)!)^{1/(N-1)}, \quad (7)$$

and we get the following result.

Corollary 1.1. *For $N \geq 3$ the inequality*

$$f_N(a_1, \dots, a_N) > ((N-1)!a_1 \cdots a_N)^{1/(N-1)} \quad (8)$$

holds.

The inequality (8) with non-strict sign was proved in [16]. The only known value of $\mu_0(S_{N-1})$ is $\mu_0(S_2) = \sqrt{3}$ (see e. g. [6]). In the latter case we get the following slight generalization of Theorems 2.2 and 2.3 in [4].

Corollary 1.2. *For $N = 3$ the inequality*

$$f_3(a_1, a_2, a_3) \geq (3a_1a_2a_3)^{1/2}$$

holds. Moreover, for any $\epsilon > 0$ and for any point $\alpha = (\alpha_1, \alpha_2)$ in \mathbb{R}^2 there exist integers $0 < a_1 < a_2 < a_3$ with $\text{GCD}(a_1, a_2, a_3) = 1$ such that

$$\left| \alpha_i - \frac{a_i}{a_3} \right| < \epsilon, \quad i = 1, 2$$

and

$$f_3(a_1, a_2, a_3) < ((3 + \epsilon)a_1a_2a_3)^{1/2}.$$

Let us consider a lattice M in \mathbb{R}^{N-1} generated by the vectors

$$\frac{1}{N-1}\mathbf{e}_1, \dots, \frac{1}{N-1}\mathbf{e}_{N-1}, \quad (9)$$

where \mathbf{e}_j are the standard basis vectors. Since the fundamental cell of M w. r. t. the basis (9) belongs to S_{N-1} , the lattice M is a covering lattice for the simplex S_{N-1} . Therefore, by (4) and (6),

$$\mu_0(S_{N-1}) \leq \frac{1}{(\det M)^{1/(N-1)}} = N-1.$$

This implies the following result.

Corollary 1.3. *For any $\epsilon > 0$ and for any point $\alpha = (\alpha_1, \dots, \alpha_{N-1})$ in \mathbb{R}^{N-1} there exist N integers $0 < a_1 < a_2 < \dots < a_N$ with $\text{GCD}(a_1, \dots, a_N) = 1$ such that*

$$\left| \alpha_i - \frac{a_i}{a_N} \right| < \epsilon, \quad i = 1, 2, \dots, N-1$$

and

$$\frac{f_N(a_1, \dots, a_N)}{(a_1 \cdots a_N)^{1/(N-1)}} < N-1+\epsilon.$$

Remark 1.2. Note that the inequality (7) and Stirling's formula imply that

$$\liminf_{N \rightarrow \infty} \frac{\mu_0(S_{N-1})}{N-1} \geq e^{-1}.$$

Thus, we know the asymptotic behavior of the optimal constant $\mu_0(S_{N-1})$ up to the multiple e .

For $\mathbf{a} = (a_1, a_2, \dots, a_N)$, define a lattice $L_{\mathbf{a}}$ by

$$L_{\mathbf{a}} = \{(x_1, \dots, x_{N-1}) : x_i \text{ integers and } \sum_{i=1}^{N-1} a_i x_i \equiv 0 \pmod{a_N}\}.$$

The following theorem is implicit in [18].

Theorem 1.2. *For any lattice L with basis $\mathbf{b}_1, \dots, \mathbf{b}_{N-1}$, $\mathbf{b}_i \in \mathbb{Q}^{N-1}$, $i = 1, \dots, N-1$ and for all rationals $\alpha_1, \dots, \alpha_{N-1}$ with $0 < \alpha_1 \leq \alpha_2 \leq \dots \leq \alpha_{N-1} \leq 1$, there exists an infinite arithmetic progression \mathcal{P} and a sequence*

$$\mathbf{a}(t) = (a_1(t), \dots, a_{N-1}(t), a_N(t)) \in \mathbb{Z}^N, t \in \mathcal{P},$$

such that $\text{GCD}(a_1(t), \dots, a_{N-1}(t), a_N(t)) = 1$ and the lattice $L_{\mathbf{a}(t)}$ has a basis

$$\mathbf{b}_1(t), \dots, \mathbf{b}_{N-1}(t)$$

with

$$\frac{b_{ij}(t)}{dt} = b_{ij} + O\left(\frac{1}{t}\right), \quad i, j = 1, \dots, N-1, \tag{10}$$

where $d \in \mathbb{N}$ is such that $d b_{ij}, d \alpha_j b_{ij} \in \mathbb{Z}$ for all $i, j = 1, \dots, N-1$. Moreover,

$$a_N(t) = \det(L)d^{N-1}t^{N-1} + O(t^{N-2}) \tag{11}$$

and

$$\alpha_i(t) := \frac{a_i(t)}{a_N(t)} = \alpha_i + O\left(\frac{1}{t}\right). \tag{12}$$

For completeness, we give a proof of Theorem 1.2 in Section 4.

2 Proof of Theorem 1.1 (i)

Recall that $\mathbf{a} = (a_1, a_2, \dots, a_N)$ and put

$$\alpha_1 = \frac{a_1}{a_N}, \dots, \alpha_{N-1} = \frac{a_{N-1}}{a_N}.$$

Define a simplex $S_{\mathbf{a}}$ by

$$S_{\mathbf{a}} = \{(x_1, \dots, x_{N-1}) : x_i \geq 0 \text{ reals and } \sum_{i=1}^{N-1} a_i x_i \leq 1\}.$$

Theorem 2.5 of [12] states that

$$f_N(a_1, \dots, a_N) = \mu(S_{\mathbf{a}}, L_{\mathbf{a}}). \quad (13)$$

Observe that the inhomogeneous minimum $\mu(S, L)$ satisfies

$$\mu(S, tL) = t\mu(S, L),$$

$$\mu(tS, L) = t^{-1}\mu(S, L).$$

Thus, if we define

$$S_{\alpha} = a_N S_{\mathbf{a}} = \{(x_1, \dots, x_{N-1}) : x_i \geq 0 \text{ reals and } \sum_{i=1}^{N-1} \alpha_i x_i \leq 1\},$$

$$L_u = a_N^{-1/(N-1)} L_{\mathbf{a}}$$

then

$$\mu(S_{\mathbf{a}}, L_{\mathbf{a}}) = a_N^{1+1/(N-1)} \mu(S_{\alpha}, L_u). \quad (14)$$

Note that $\det L_{\mathbf{a}} = a_N$. Thus the lattice L_u has determinant 1 and we have

$$\mu_0(S_{\alpha}) \leq \mu(S_{\alpha}, L_u). \quad (15)$$

The simplices $(\alpha_1 \cdots \alpha_{N-1})^{1/(N-1)} S_{\alpha}$ and S_{N-1} are equivalent up to a linear transformation of determinant 1. Therefore

$$\mu_0(S_{N-1}) = \frac{\mu_0(S_{\alpha})}{(\alpha_1 \cdots \alpha_{N-1})^{1/(N-1)}}, \quad (16)$$

and by (15), (14) and (13) we have

$$\begin{aligned} \mu_0(S_{N-1}) &\leq \frac{\mu(S_{\alpha}, L_u)}{(\alpha_1 \cdots \alpha_{N-1})^{1/(N-1)}} = \frac{\mu(S_{\mathbf{a}}, L_{\mathbf{a}})}{a_N^{1+1/(N-1)} (\alpha_1 \cdots \alpha_{N-1})^{1/(N-1)}} \\ &= \frac{f_N(a_1, \dots, a_N)}{(a_1 \cdots a_N)^{1/(N-1)}}. \end{aligned}$$

3 Proof of Theorem 1.1 (ii)

The proof is based on Theorem 1.2 and the following continuity property of the inhomogeneous minima. We say that a sequence S_t of *star bodies* in \mathbb{R}^{N-1} converges to a star body S if the sequence of *distance functions* of S_t converges uniformly on the unit ball in \mathbb{R}^{N-1} to the distance function of S .

Lemma 3.1. *Let S_t be a sequence of star bodies in \mathbb{R}^{N-1} which converges to a bounded star body S and let L_t be a sequence of lattices in \mathbb{R}^{N-1} convergent to a lattice L . Then*

$$\lim_{t \rightarrow \infty} \mu(S_t, L_t) = \mu(S, L).$$

Proof. The result follows from a much more general Satz 1 of [10]. \square

W. l. o. g., we may assume that $\alpha \in \mathbb{Q}^{N-1}$ and

$$0 < \alpha_1 < \alpha_2 < \dots < \alpha_{N-1} < 1. \quad (17)$$

For $\epsilon > 0$ we can choose a lattice L_ϵ of determinant 1 with

$$\mu(S_\alpha, L_\epsilon) < \mu_0(S_\alpha) + \frac{\epsilon(\alpha_1 \cdots \alpha_{N-1})^{1/(N-1)}}{2}. \quad (18)$$

The inhomogeneous minimum is independent of translation and rational lattices are dense in the space of all lattices. Thus, by Lemma 3.1, we may assume that $L_\epsilon \subset \mathbb{Q}^{N-1}$. Applying Theorem 1.2 to the lattice L_ϵ and the numbers $\alpha_1, \dots, \alpha_{N-1}$, we get a sequence $\mathbf{a}(t)$, satisfying (10), (11) and (12). Note also that, by (17),

$$0 < a_1(t) < a_2(t) < \dots < a_N(t)$$

for sufficiently large t .

Observe that the inequality (12) implies (2) with $a_i = a_i(t)$, $i = 1, \dots, N$, for t large enough. Let us show that, for sufficiently large t , the inequality (3) also holds. Define a simplex $S_{\alpha(t)}$ and a lattice L_t by

$$S_{\alpha(t)} = a_N(t) S_{\mathbf{a}(t)} = \{(x_1, \dots, x_{N-1}) : x_i \geq 0 \text{ reals and } \sum_{i=1}^{N-1} \alpha_i(t) x_i \leq 1\},$$

$$L_t = a_N(t)^{-1/(N-1)} L_{\mathbf{a}(t)}.$$

By (10) and (11), the sequence L_t converges to the lattice L_ϵ . Next, the point $\mathbf{p} = (1/(2N), \dots, 1/(2N))$ is an inner point of the simplex S_α and all the simplices $S_{\alpha(t)}$ for sufficiently large t . By (12) and Lemma 3.1, the sequence $\mu(S_{\alpha(t)} - \mathbf{p}, L_t)$

converges to $\mu(S_\alpha - \mathbf{p}, L_\epsilon)$. Since the inhomogeneous minimum is independent of translation, the sequence $\mu(S_{\alpha(t)}, L_t)$ converges to $\mu(S_\alpha, L_\epsilon)$. Consequently, by (12),

$$\frac{\mu(S_{\alpha(t)}, L_t)}{(\alpha_1(t) \cdots \alpha_{N-1}(t))^{1/(N-1)}} \rightarrow \frac{\mu(S_\alpha, L_\epsilon)}{(\alpha_1 \cdots \alpha_{N-1})^{1/(N-1)}}, \text{ as } t \rightarrow \infty,$$

and, by (13), (18) and (16),

$$\frac{f_N(a_1(t), \dots, a_N(t))}{(a_1(t) \cdots a_N(t))^{1/(N-1)}} = \frac{\mu(S_{\alpha(t)}, L_t)}{(\alpha_1(t) \cdots \alpha_{N-1}(t))^{1/(N-1)}} < \mu_0(S_{N-1}) + \epsilon$$

for sufficiently large t .

4 Proof of Theorem 1.2

Let us consider the matrices

$$B = \begin{pmatrix} b_{11} & b_{12} & \dots & b_{1N-1} & \sum_{i=1}^{N-1} \alpha_i b_{1i} \\ b_{21} & b_{22} & \dots & b_{2N-1} & \sum_{i=1}^{N-1} \alpha_i b_{2i} \\ \vdots & \vdots & & \vdots & \vdots \\ b_{N-11} & b_{N-12} & \dots & b_{N-1N-1} & \sum_{i=1}^{N-1} \alpha_i b_{N-1i} \end{pmatrix}$$

and

$$M = M(t, t_1, \dots, t_{N-1})$$

$$= \begin{pmatrix} db_{11}t + t_1 & db_{12}t & \dots & db_{1N-1}t & d \sum_{i=1}^{N-1} \alpha_i b_{1i}t \\ db_{21}t & db_{22}t + t_2 & \dots & db_{2N-1}t & d \sum_{i=1}^{N-1} \alpha_i b_{2i}t \\ \vdots & \vdots & & \vdots & \vdots \\ db_{N-11}t & db_{N-12}t & \dots & db_{N-1N-1}t + t_{N-1} & d \sum_{i=1}^{N-1} \alpha_i b_{N-1i}t \end{pmatrix}.$$

Denote by $M_i = M_i(t, t_1, \dots, t_{N-1})$ and B_i the minors obtained by omitting the i th column in M or in B , respectively. Following the proof of Theorem 2 in [18], we observe that

$$|B_N| = |\det(b_{ij})| = \det L, \tag{19}$$

$$|B_i| = \alpha_i |B_N|, \tag{20}$$

$$M_i = d^{N-1} B_i t^{N-1} + \text{polynomial of degree less than } N-1 \text{ in } t, \tag{21}$$

and M_1, \dots, M_N have no non-constant common factor.

By Theorem 1 of [18] applied with $m = 1$, $F = 1$, and $F_{1\nu} = M_\nu(t, t_1, \dots, t_{N-1})$, $\nu = 1, \dots, N$, there exist integers t_1^*, \dots, t_{N-1}^* and an infinite arithmetic progression \mathcal{P} such that for $t \in \mathcal{P}$

$$\text{GCD}(M_1(t, t_1^*, \dots, t_{N-1}^*), \dots, M_N(t, t_1^*, \dots, t_{N-1}^*)) = 1.$$

Put

$$\mathbf{a}(t) = (M_1(t, t_1^*, \dots, t_{N-1}^*), \dots, (-1)^{N-1} M_N(t, t_1^*, \dots, t_{N-1}^*)) , \quad t \in \mathcal{P}.$$

Then the basis $\mathbf{b}_1(t), \dots, \mathbf{b}_{N-1}(t)$ for $L_{\mathbf{a}(t)}$ satisfying the statement of Theorem 1.2 is given by the rows of the matrix obtained by omitting the N th column in the matrix $M(t, t_1^*, \dots, t_{N-1}^*)$. The properties (19)–(21) of minors M_i , B_i imply the properties (10)–(12) of the sequence $\mathbf{a}(t)$, $t \in \mathcal{P}$.

Acknowledgement. The authors are especially grateful to Professors M. Henk and A. Schinzel for important comments and remarks that strongly improve the exposition. The authors also wish to thank Professors I. Cheltsov, L. Fukshansky, L. Davison and J. Ramirez Alfonsin for very helpful and useful discussions.

References

- [1] R. P. Bambah, *On Lattice Coverings*, Proc. Nat. Inst. Sci. India, **19** (1953), 447–459.
- [2] M. Beck, R. Diaz, S. Robins, *The Frobenius Problem, Rational Polytopes, and Fourier-Dedekind sums*, J. Number Theory, **96** (2002), no. 1, 1–21.
- [3] W. J. Curran Sharp, *Solution to Problem 7382* (Mathematics), Educational Times, **41** (1884).
- [4] J. L. Davison, *On the Linear Diophantine Problem of Frobenius*, J. Number Theory, **48** (1994), no. 3, 353–363.
- [5] P. Erdős, R. Graham, *On a Linear Diophantine Problem of Frobenius*, Acta Arith., **21** (1972), 399–408.
- [6] I. Fáry, *Sur la Densité des Réseaux de Domaines Convexes*, Bull. Soc. Math. France, **78**(1950), 152–161.
- [7] L. Fukshansky, S. Robins, *Frobenius Problem and the Covering Radius of a Lattice*, submitted.
- [8] H. Greenberg, *Solution to a Linear Diophantine Equation for Nonnegative Integers*, J. Algorithms, **9** (1988), no. 3, 343–353.

- [9] R. K. Guy, Unsolved Problems in Number Theory, Third edition. Problem Books in Mathematics. Unsolved Problems in Intuitive Mathematics, Springer-Verlag, New York, 2004.
- [10] P. Gruber, *Zur Gitterüberdeckung des \mathbb{R}^n durch Sternkörper*, Österreich. Akad. Wiss. Math.-Natur. Kl. S.-B. II, **176** (1967), 1–7.
- [11] P. M. Gruber, C. G. Lekkerkerker, *Geometry of Numbers*, North-Holland, Amsterdam 1987.
- [12] R. Kannan, *Lattice Translates of a Polytope and the Frobenius Problem*, Combinatorica, **12**(2)(1992), 161–177.
- [13] R. Kannan, L. Lovász, *Covering Minima and Lattice-Point-Free Convex Bodies*, Ann. of Math. (2) **128** (1988), no. 3, 577–602.
- [14] J. L. Ramírez Alfonsín, *The Diophantine Frobenius Problem*, Oxford Lecture Series in Mathematics and Its Applications, 2005.
- [15] O. Rödseth, *On a Linear Diophantine Problem of Frobenius*, J. Reine Angew. Math., **301** (1978), 171–178.
- [16] O. Rödseth, *An upper bound for the h-range of the postage stamp problem*, Acta Arith., **54** (1990), no. 4, 301–306.
- [17] C. A. Rogers, *Packing and Covering*, Cambridge Tracts in Mathematics and Mathematical Physics, No. 54 Cambridge University Press, New York 1964.
- [18] A. Schinzel, *A Property of Polynomials with an Application to Siegel's Lemma*, Monatsh. Math., **137** (2002), 239–251.
- [19] E. Selmer, *On the Linear Diophantine Problem of Frobenius*, J. Reine Angew. Math., **293/294** (1977), 1–17.
- [20] E. Selmer, O. Beyer, *On the Linear Diophantine Problem of Frobenius in Three Variables*, J. Reine Angew. Math., **301** (1978), 161–170.
- [21] Y. Vitek, *Bounds for a Linear Diophantine Problem of Frobenius*, J. London Math. Soc., (2) **10** (1975), 79–85.

School of Mathematics, University of Edinburgh, Edinburgh EH9 3JZ, UK, I.Aliev@ed.ac.uk

Technische Universität Wien, Wiedner Hauptstrae 8-10 / 1046, 1040 Wien, Austria,
peter.gruber@tuwien.ac.at